# Computer use policy

OFFICE OF RAIL REGULATION

## Purpose

1. The purpose of this policy is to provide clear rules and guidelines on internal and external computer use, when using Office of Rail Regulation (ORR) computer systems.

2. The policy underpins the Conduct Policy which sets out the standards of behaviour expected from ORR employees.

## Scope

3. This policy applies to all permanent and fixed-term employees at all grades of staff throughout ORR. It also applies to temporary employees – casual staff, agency staff, secondees and consultants – who are provided with access to ORR computer systems.

4. Throughout this policy the term “ORR computer systems” or “computer systems” should be read as including: standalone computers; computers provided by ORR for use at home; computer software including e-mail and internet software; laptops; handheld devices including Blackberry handsets; and any other ancillary equipment such as servers, scanners etc.

## Responsibility

5. All employees referred to within the scope of this policy are required to adhere to its terms and conditions and must understand that this policy is also incorporated into their contract of employment. **Employees must sign the declaration (at Annex B) and confirm they have read and understand this policy and their responsibilities each time they log-on to an ORR computer.**

6. Line managers are responsible for ensuring that this policy is applied within their own area. It is also the responsibility of managers to inform any consultant or temporary staff they are responsible for that ORR has a computer use policy and to ensure that they have read and understood the policy and their responsibilities.

7. HR will monitor the application of this policy. Any queries on the application or interpretation of this policy must be discussed with HR or the IS team prior to any action being taken.

## Policy statement

8. Computers are essential and powerful tools that help employees to do their work and employees should not hesitate to use them in their day-to-day work. However, employees need to understand the rules and standards of conduct to be followed when using computers.

9. It is the intention of ORR to encourage responsible use of e-mail, the Intranet and the Internet. Compliance with this policy will help prevent damage to, and misuse of, ORR

computer systems and protect our staff and external stakeholders from the possible consequences of such misuse. Failure to comply with the policy may result in:

(a) legal claims against individuals and/or ORR; and/or

(b) disciplinary action being taken against individuals, which could result in dismissal; and /or

(c) prosecution for a criminal offence.

10. Employees must remember that every document written on ORR computer system, including e-mails, can be recovered (even if it has been deleted). Computer documents may be used as evidence at a future date, for example in a hearing or judicial review or if a breach of any HR policy is being investigated. Therefore, employees must be mindful of what they write in all computer documents – including e-mails, as an e-mail constitutes correspondence rather than a conversation and is therefore capable of being considered as the same as a formal memorandum.

11. All computer systems are provided for ORR business, and employees must never use them in any way that interferes with or impedes official business.

12. Employees should ensure that the e-mails they send to others meet the requirements of ORR's Conduct Policy. Care should be taken with the style, language and tone used, and the sender must consider the effect that the message may have on the recipient.

13. Direct 'face-to-face' or verbal communication should be used if it is likely that an e-mail message may be misunderstood or misinterpreted. If an issue is detailed or complex then it should preferably be set out in a formal letter or memorandum (which can then be sent as an attachment to an e-mail) and not in the body of an e-mail.

14. Employees must remember that, although the sender and/or the receiver can delete e-mail, it will still be retrievable if required.

15. The reasonable use of computer systems is acceptable for recognised ORR bodies, such as Staff Representative Group (SRG) or social committee work provided it does not interfere with ORR business.

## Unacceptable use of ORR computer systems

16. ORR is committed to promoting an environment of equality and diversity. All employees (whether permanent or temporary) **must not** use the computer systems for any purpose that could be regarded as contrary to ORR's Equality and Diversity policy or discriminatory on the grounds of: race, colour, nationality, ethnic or national origin; sex or sexual orientation; gender reassignment; marital status; working pattern; religion or cultural background; disability; or age.

17. Misuse of ORR computer systems will be regarded as particularly serious if it is likely to bring ORR into disrepute. This includes anything that contravenes the law, including: the Official Secrets Act (1989); the Computer Misuse Act (1990); the Data Protection Act (1998); any equal opportunities legislation; and any obscenity, defamation or copyright laws.

18. Some uses are **absolutely unacceptable to ORR**: for example, accessing pornography, gambling websites, extreme political causes, racist websites etc.

## Monitoring

19. In order to ensure the effective operation of this policy and to safeguard ORR's greater interests (whilst also being mindful of the general right of employees to privacy at work) ORR reserves the right to monitor the use of Internet websites and e-mails sent by any of its employees. This includes e- mails sent from their PC to other employees internally and also to other people externally. ORR also reserves the right to monitor e-mails sent to any of its employees at their ORR e-mail address.

20. Employees may use ORR computer systems for personal purposes subject to the conditions set out in this policy (at paragraphs 32 - 36 below). However, employees should be aware that the use of ORR computer systems is monitored - **employees cannot, therefore, have any expectation of privacy if they use ORR computer systems for personal purposes**.

21. ORR will monitor aspects such as frequency and duration of employees' access to an encrypted site, such as an Internet banking site, but is not able to monitor the content of, or transactions within that site.

22. All monitoring will be carried out in accordance with this policy and what is permitted by law. ORR will monitor the computers systems to:

(a) ensure compliance with this policy, IS practices and procedures;

(b) prevent or detect crime; and

(c) investigate or detect misconduct, including gross misconduct, through unacceptable/unauthorised use of the computer systems.

23. ORR will inform employees of any changes to the policy on monitoring before they are implemented.

## E-mail monitoring

24. ORR will log all e-mail traffic to monitor the performance and capacity of the system. These activity logs can also be used to monitor an individual's use of the e-mail system. An employee's e-mail use will only be monitored if misuse of the system or criminal activity is suspected. All such monitoring will be authorised by the Head of HR.

25. The email use of **all** employees might be monitored to inform an office- wide security / audit investigation. On these occasions the monitoring will be initiated by the Audit Committee or by the Chief Executive (on the advice of the IS team). Before any such monitoring begins, employees will be told that an audit is being carried out, and justification for that audit will be provided.

26. In the course of their day-to-day management function, line managers **may sometimes need access to their staff's mailboxes - for example, if the** employee is off sick or on leave. However, in such circumstances line managers must not deliberately access e-mails that are clearly personal.

27. If a line manger needs to obtain access to an employee's computer for legitimate reasons then the following procedure will be followed:

(a) the line manager will e-mail a request for access to IS Servicedesk and copied to the employee's e-mail address;

(b) IS Servicedesk will reset the user account password and notify the line manager;

(c) The line manager must tell the employee when they return to work that they have accessed their computer and why, and that the password has been changed; and

(d) The employee should then change the password to a new password.

## Internet monitoring

28. ORR employees are protected against accessing inappropriate websites by a combination of internet monitoring software and hardware firewalls. These tools refuse access to certain sites that may contain inappropriate or illegal information. If an employee wishes to access a particular website that is restricted then they can request access by using the form at

**Annex A**. The request will be evaluated by the IS team in discussion with line managers and HR and may be declined if access to the site is considered to be an inappropriate use of ORR computer systems.

29. ORR's computer systems will automatically keep logs of all Internet websites visited, and by whom. These logs will be retained for up to 12 months (unless the logs form part of an investigation), and will be checked regularly by the IS team to see whether any unacceptable sites have been accessed by employees.

30. If the IS team finds evidence of visits to unacceptable sites, or other unauthorised use of the Internet, details will be sent to the Head of HR for investigation.

31. It is part of a line manager's role to be continually aware of their staff's performance and of any factors that may be adversely affecting it. Line managers should observe their staff's use of the Internet (and e-mail) in the same way as they do, for example, personal use of the telephone at work. If they see that personal use is excessive or inappropriate this is, in the first instance, a management issue that should be dealt with through informal cautions (see Discipline Policy).

## Personal use

32. A reasonable degree of responsible personal use is allowed, subject to the conditions set out in this policy. Every employee is expected to exercise good judgement and keep the majority of their personal use of ORR computer systems to either before they start work, during their lunchtime, or after work.

33. However, it is recognised that there may be occasions when employees need to use the e-mail or internet for personal use during work time – this is acceptable if:

(a) The personal use is brief and occasional; and

(b) The line manager is aware that the employee might be using the computer for brief and occasional personal use during working hours, and is content that this will not have a detrimental effect on the employee's work and/or performance.

34. Personal use includes, but is not limited to, sending and receiving personal e-mails, accessing the Internet and using the computer software (such as for writing personal letters etc). It is unacceptable, however, for employees to use ORR computer systems in relation to running a personal business at any time.

35. **Personal use of ORR computer systems is a benefit, which may be withdrawn from employees where line managers consider it is appropriate to do so.**

## Disclaimer for personal use of equipment and services

36. ORR allows employees to use the internet and e-mail services for personal use on the understanding that this is at the discretion of management and, subject to this policy, ORR will not be liable in any way for any losses, damages, costs or expenses of any kind arising directly or indirectly from the use of, or the inability to use, ORR computer systems and/or licensed software programmes.

### Examples of computer misuse

37. The following lists are not exhaustive – they are for guidance only. It should not be assumed that the absence of a particular activity or behaviour from these lists would make it acceptable.

38. The following examples of serious misuse will be considered as **gross misconduct**, and will be dealt with as such under the Discipline Policy:

(a) Employees must not import or send any e-mail message or attachment that could be construed as obscene, abusive, libellous, racist, offensive or amounting to prejudice or harassment of any kind;

(b) Employees must not visit illegal or unacceptable web sites such as those containing material that is pornographic[1], racist, in breach of copyright, or contain details of how to undertake computer hacking;

(c) Employees must not print, open pages, and/or send on material from illegal or unacceptable sites. *NB. This could constitute a criminal offence*;

(d) Employees must not impersonate any other person when using e-mail, or amend messages received from others;

(e) Employees must not allow their use of e-mail and the Internet to have the potential to harm ORR's reputation;

(f) Employees must not undertake activities for commercial gain, for example, in connection with a business run by themselves or a partner; and

(g) Employees must not send classified, sensitive or otherwise potentially damaging material to an unauthorised person.

39. The following examples of misuse are unacceptable and should be avoided. However, breaches will not be treated as gross misconduct unless the line manager has given clear cautions that the employee's behaviour is unacceptable and the unacceptable use continues:

(a) Employees must not excessively use e-mail or the internet for personal reasons during work time;

(b) Employees must not send internal e-mails to a large number of people if it is not business related **unless** the e-mail is from the social committee, SRG, or trade union, or is an announcement about an employee (e.g. births, birthdays, a presentation etc.);

(c) Employees must not send ORR business-related e-mails to 'everyone' if that is not the appropriate audience;

(d) Employees must not respond to 'spam' e-mails as this encourages further 'spam';

(e) Employees must not use swear words or offensive language in e-mails;

(f) Employees must not send or forward e-mail chain letters;

(g) Employees must not send greeting cards as these are graphics files so have a detrimental effect on the speed of the network;

(h) Employees must not undertake share dealing, or gambling;

(i) Employees must not subscribe to chat rooms (including business- related chat rooms);

(j) Employees must not use their official e-mail address to subscribe to Internet services, such as information services, bulletin boards, newsgroups, except for business related reasons;

(k) Employees must not post information to external newsgroups or bulletin boards in their official capacity or from their official address unless their duties specifically authorise them to do so;

[1] Pornographic in this context means not only obscene or indecent material that, it is an offence to possess or publish, but also "soft porn" such as images of nudity and similar material that might cause distress or offence to an employee.

(l) Employees must not buy goods or services for business use over the Internet unless they are authorised to do so;

(m) Employees must not use someone else's password or give their password to someone else;

(n) Employees must use 'complex' passwords containing a combination of upper and lower case letters and a mix of letters and numbers. Blackberry users must comply with the password requirements set out in the Blackberry User Security Guidance;

(o) Employees must not use an inappropriate or offensive screensaver; and

(p) Employees must not use the audio/sound facility during working time (unless it is necessary for a work-related reason and/or with the line manager's agreement).

## Notification of accidental misuse

40. If an employee is the recipient of wholly unacceptable computer material, accidentally accesses a website that might be considered wholly unacceptable or becomes aware of serious computer misuse by some other means, they must tell a senior manager in their team (*i.e.* no lower than a grade A) and the Head of HR immediately.

41. An employee should directly notify their line manager and the IS Servicedesk if they receive suspect computer material, so that the reporting of the incident is electronically recorded (to protect the employee) and appropriate or remedial action can be taken immediately to protect other employees.

## Action taken against people who misuse ORR computer systems

42. Any computer use that ORR considers unacceptable will be regarded as unauthorised use of the computer systems. If an employee is in any doubt about what constitutes unacceptable computer use they should send a written query (preferably e-mail) to their line manager, who should then provide a written response. The line manager can seek additional advice from the IS team or the HR team as necessary. This enables the employee to demonstrate that they have made every effort to clarify whether their activities are acceptable to ORR.

43. Employees must be given clear cautions by their line manager if their use of the computer systems is unacceptable and, if they continue to use the computer systems in such a way, might result in disciplinary action being taken against them. Any continued serious misuse following a caution will be treated as **gross misconduct.**

44. All suspected serious misuse of ORR computer systems that might be considered as gross misconduct will be investigated thoroughly and dealt with through the ORR Discipline Policy.

45. If a line manager has grounds for suspecting serious misuse of e-mail or the Internet by an employee then they must send a written request for a formal investigation to take place to the Head of HR, giving full written details of the grounds of their suspicion together with all available evidence and any action taken so far.

46. If the Head of HR considers the circumstances sufficiently serious they will initiate a thorough investigation, following the procedure as set out in the Discipline Policy. This will include a review of the employee's computer log.

47. Any disciplinary action taken as a result of an investigation will depend on the seriousness of the offence.

48. Each case will be decided on its own merits and due consideration will be given to any

mitigating factors. The range of penalties will include, but is not restricted to:

(a) formal disciplinary warnings;

(b) sanctions such as a ban on using ORR computer systems for personal use;

(c) downgrading; and

(d) dismissal.

49. **Employees must be aware that serious computer misuse will be subject to action under the Discipline Policy.** National Audit Office and Internal Audit will be informed of any disciplinary proceedings arising from alleged incidences of serious misuse. Employees must be aware that serious contravention – that is serious misuse that is found to be gross misconduct - could lead to their dismissal.

50. There is a clear distinction between a disciplinary offence that can be dealt with by ORR and a criminal offence. Internal investigations should not be allowed to prejudice the outcome of any criminal proceedings. Furthermore, ORR will have no hesitation on reporting serious misuse that could be regarded as a criminal offence to the police.

51. Any member of staff who is the victim of a criminal offence has the right to contact the police but they should also inform their line manager who will report the fact to the Head of HR.

## Maintaining this policy

52. IS has responsibility for ensuring the maintenance, regular review and updating of this policy. Revisions, amendments or alterations to the policy can only be implemented following consideration by Directors' Group and SRG, and approval by the ORR Board. Changes will be notified to employees as
and when they occur.

# Request for access to restricted website

| | |
|---|---|
| **Name:** | |
| **Access is requested to the following restricted website:**<br><br>Please provide full web address | |
| **Reason access requested:**<br><br>Please provide full details as to why you are requesting access this website, including any business justification. | |
| **Signed:** | |
| **Date:** | |

**Please now send your request to the IS Service Desk**

| | |
|---|---|
| **Head of IS:**<br><br>I authorise that: *(delete as appropriate)*<br><br>• access to this website can be granted at any time<br><br>• access to this site should not be granted | **Signed:**<br><br>**Head of IS**<br><br>**Date:** |
| **IS Service Desk:**<br><br>• Action to change restriction taken (if appropriate)<br><br>• Employee notified of change to access | **Signed:**<br><br>**Date:** |

## ANNEX B - COMPUTER USE POLICY: DECLARATION

- I have read and understand the policy regarding computer use (and misuse);
- I accept my responsibilities under the terms of this policy; and
- I understand that serious contravention of the Computer Use Policy will constitute gross misconduct, which could lead to my dismissal.

**SIGNED:**

**NAME:**

*(block capitals)*

**DATE:**